Note: The answer to question 37 was updated on 7/11/13 at 2:00pm

Questions and Answers for "Third-Party Security Assessment - Minnesota Insurance Marketplace (MNsure)" SOW

1. Is there a budget cap?
   A: We cannot provide information on the project budget, but it most certainly does have a cap. Per the SOW process, responses are scored for merit and, only after all technical/project responses are reviewed and scored, then costs proposals are evaluated for value.
2. Who is the incumbent?
   A: There is no incumbent. This is a specific multi-phase assessment engagement to examine an new Health Insurance Marketplace system.
3. Can some or all of this work be done remotely?
   A: Almost all of the work will need to completed on-site. There are systems to be assessed that are not yet available externally as well as physical location inspections and in-person interviews to conduct.
4. Can you please provide us the list of architecture components (under "Project Environment (State Resources)" section, it is stated that this would be made available upon request)
   A: All vendors that requested it received this information via encrypted email with the message that these documents are classified as non-public security information; provided to serious bidders only, and; must be destroyed when no longer needed.
5. Some vendors requested a time extension.
   A: We are not able to provide any time extensions. This project is already behind and we have very tight timelines. The dates for the exchange are set nationally by the feds. We need to have enough time to substantially mitigate any findings, and the feds need time to review the report, before our 9/1 deadline to receive Authority to Operate.
6. How many controls are expected to be tested in the assessment based on your SSP? Or are you willing to share your SSP?
   A: Our SSP is a line-by-line response to the federal MARC-E (Minimum Acceptable Risk Controls for Exchanges), http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf. This document is substantially based on NIST 800-53. Our expectation, as listed in the SOW, is that the review will be conducted on all of the controls, using the methodology outlined in NIST 800-53A and with results presented in a manner similar to the FedRAMP assessment document linked in the SOW. Since the system is still in development, it is possible that some of the controls may not be ready to test.
   Our completed SSP is classified as non-public security information and we will provide a copy of that document to the vendor chosen to provide the assessment.
7. How large is the State organization providing the insurance exchange? What is the highest total number of State users of the system by the time of the conclusion of the assessment?
   A: MNsure is a new state agency with approx. 35 staff. The Dept. of Human Services (DHS) is the primary technical team and that agency has 7000 staff. There is also a statewide IT organization called MN.IT, some of these staff are included in the DHS count.
   The system is not yet live and there are no users. The system goes live on Oct. 1 (as do all similar systems nationwide).
8. What are the addresses of the State buildings from which these employees will be working?
   A: The primary work locations are close together in downtown St. Paul – 540 Cedar Ave. (DHS) and 81 7th St. (MNsure)
9. Which roles will be assigned to this project, and for what percent of their assigned workload?

A: The overall system project is well staffed. We do not have individuals specifically assigned to assist with the security controls assessment. A security staff with architects, engineers, PM and BAs, as well as the CISO, will be available to be interviewed or otherwise answer questions. Technical staff will assure appropriate access is available. Otherwise, it is expected that the chosen vendor staff perform the actual assessment duties.

10. How many third-party organizations currently have access to the exchange as users? How many as service providers? Can you provide us the names of these third parties?
    A: The system is not yet live. The only 3rd party access is by the vendor developers working on the system. These include: IBM/Curam, Engagepoint, and Maximus.
11. How are these numbers expected to change by the end of the assessment?
    A: The system will still not be deployed by the end of phase 1 of the engagement. There could be as many as 300,000 users of the system by the end of 2013.
12. What are the different types of components, and how many of each, are there in the in-scope system? For example, a server and a firewall are examples of components.
    A: Included in the system hardware/software information sent upon request
13. About how many IP addresses are in scope?
14. Which URLs are in scope?
    A: The system architecture hardware and software lists have been sent separately. There will be one main URL which has not yet been determined. There is an existing MNsure site at http://www.mn.gov/hix/.
15. Does the exchange already store information on individuals? If so, on approximately how many millions of individuals?
    A: There is not yet any production data on individuals in the system. Once the system is given federal "Authority to Connect/Authority to Operate" the system will connect to the federal hub and contain production data.
16. How would you characterize the level of completeness of the exchange's documentation of its information-security policies? Of its information-security standards and procedures?
    A: The SSP, which has been submitted to the federal government, contains a very complete set of policies, standards, procedures and guidelines, as well as the state's plans to meet the control requirements listed in the MARC-E, http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf.
17. Has the State experienced past data breaches involving the exchange? If so, what were the nature of those breaches?
    A: The exchange is a new system and will go live on Oct. 1. There are very stringent breach notification laws surrounding health insurance exchanges.
18. Has the State already conducted network-vulnerability scans? Application-vulnerability scans? Does the State want the vendor to include these scans in scope?
    A: The system is included in our continuous vulnerability scans. In addition, each software component has undergone application security scanning. The vendor must test whether the state has met the controls listed in the SSP (which includes assessing that our application and vulnerability scanning programs are sufficient).
19. What organizational or technical changes are still undecided at this point involving the exchange, but may be decided once the project is launched? For example, are key vendors or architectural decisions still outstanding?
    A: This is a constantly shifting project as the federal authorities continue to make changes. However, the assessment centers on: a) does the state SSP responses meet the requirements of the MARC-E, and; b) has the state implemented the controls stated in the SSP.

20. How important will specific IRS/HIPAA/privacy/security audit experience be in the selection process?
    A: Each of the criteria listed for the vendor selection will be equally scored. So this item is just one of many. Overall we're looking for experience in dealing with various fed regulatory requirements. Our guiding requirements doc, the MARC-E, http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf, draws from various regulations, but is primarily based on 800-53.
21. The RFP also states that we should have familiarity with MNsure. Since this is relatively new, we would not have had an opportunity to have direct experience with this. How important is this?
    A: Again, this is just one of a list of criteria. We are looking for a vendor who has some understanding of the regulations and challenges that are affecting exchanges. Since there are not yet any exchanges really up and operating, we're not expecting actual hands-on experience with a fully operating exchange. But knowledge of the components is useful.
22. What FIPS-199 classification category applies to the department, (High, Medium or Low)?
    A: The feds consider the exchanges to require Moderate/Medium controls. That is reflected in our SSP.
23. Who will consume this report, i.e. will the results only be distributed internally within the State in order to make the needed adjustments or will 3rd parties have access to the results?
    A: The results will be used by internal security and technical staff and must be provided to the feds to be used in consideration, with our other documentation, for our request for Authority to Operate. Otherwise, the report is classified as non-public security information and will not be shared further.
24. Opinion vs. Recommendation: Is the work in this SOW preparatory work for another firm that will go on and perform attestation? (As an accounting firm, we look at the word "opinion" as having a very specific meaning.)
    A: No. We used the word "opinion" to mean that we expect the vendor to do more than simply complete a checklist. We want this overall "endorsement" (for lack of a better word) based on the vendors expertise that the state has (or has not) done a good job both in interpreting and implementing the required controls from a compliance standpoint AND has (or has not) created a strong security environment for this system.
25. Will the application be covered under current security policies established and implemented by the State of MN, or will there be a dedicated set of policies created expressly for the application. On average, how many documents / pages per document will the State provide for the assessment?
    A: A new security policy/standard deck was created based on the specific fed requirements of this project. It's all based on 800-53 and these new policies/standards will become the new statewide policies/standards.
26. Does the risk assessment need to include independent validation of controls, or will an interview / documentation review be sufficient?
    A: We do need technical verification of an appropriate set of the controls.
27. If control validation is required, what is the desired sampling methodology? How many systems / types of systems will be in scope for the assessment?
    A: We expect the assessment to follow 800-53A, but otherwise want the vendor to make recommendations on other specifics. The overall system is still in development and changing. The hardware/software inventory provides size info.
28. Does the state require that an assessment against MARS-E and NIST 800-53A be performed multiple times throughout the project in order to update the results with remediation activities?
    A: That is what is covered in the multi-phase plan, both to track remediation as well as code and feature updates.
29. What is the makeup of technology involved in supporting the new application? Please, provide:
    Server platform

Database platform
Software development language
Other critical technologies
A: See the hardware/software inventory appendices.

30. Anonymous Network & Application Layer Penetration Testing:
    Number of active IP addresses?
    Number of URLs or Web-applications in scope?
    A: I don't have this info. The system is only internally accessible right now and only fully lives in a dev environment. There is one main portal and the rest of the system is made up of a series of COTS products integrated network, storage and tools in a SOA environment.
31. Network Architecture and FW Review:
    How many device configs need to be reviewed (generally routers and firewalls, please provide make/model)? any switches, bridges, wireless, or any other devices need configuration review?
    A: The assessment will focus inside of the system boundary, though a basic look at the network path to the system boundary is in scope.
32. Total approximate number of ACLs/Policies?
    A: I don't have this info, though there is only basic portal interface plus a separate b2b interface to the system.
33. Any policy review in scope? if so, how many pages of documentation?
    A: The assessment revolves around showing that: a) the state's SSP provides appropriate controls for the system; b) the state has actually implemented what is listed in the SSP, and; c) providing an overall opinion that the state has chosen and implemented appropriate controls for the system.
34. Is virtual architecture in scope? Is Storage architecture in scope?
    A: Only as part of the overall opinion. If there are any major issues we want to know, but these are effectively fixed.
35. How many physical locations need to be reviewed?
    A: The system components all reside in 2 state data centers, one in the Capitol complex in St. Paul and another nearby. Staff working on this system reside in one of 3 buildings within a few blocks in the Capitol complex in St. Paul.
36. Web-app questions:
    How many applications are in scope?
    Is the testing only from an external perspective? If yes, how many web-applications or urls are in scope?
    Will this be only unauthenticated testing? Or, will there be authenticated testing?
    If authenticated testing is in scope, will the testing be done on a replicated test environment or in production environment?
    If authenticated testing is in scope, how many applications will be tested? Are they web-input form apps, web-services, flash components?
    Number of User-profiles (user, super-user, admin)
    How many web-input forms or web-service methods?
    What is the code-base?
    How many lines of code?
    Is code base available to test to enhance the application penetration test?
    A: I'll try to answer these as a group. There are 4 main COTS products plus various tools, databases and infrastructure within the system boundary. All applications have undergone, or will undergo, application-level vulnerability testing via a state-owned tool. It is not necessarily expected that the vendor will repeat this work. The hardware/software inventory provides the sizing of the system. Otherwise, the state expects the engagement to follow the methodology in 800-53A. The vendor response can certainly recommend additional methodology.

37. With respect to the cost portion of the SOW response requirements, is MNsure seeking hourly billing rate(s) for the proposed resource(s), or is MNsure seeking a fixed-price cost proposal to complete the deliverables outlined in the SOW?
    A: The State is looking for the overall cost for completion of the project, however in order to meet program requirement you will need to break down the estimated number of hours per deliverable and the associated hourly rates which must be in line with your contract rates. **(updated 7/11/13 at 2:00 pm)**
38. If MNsure is looking to secure these resources on a "Staff Augmentation" basis, please confirm that it will be acceptable for vendors to provide hourly billing rates along with resumes in order to satisfy the "Cost" requirement?
    A: This is not a staff augmentation engagement but a specific security assessment engagement.
39. Please confirm whether selected vendor will be paid on an hourly basis for services provided under this contract, based on MNsure approved contractor time sheets, or if selected vendor will be paid based on completed/signed-off deliverables?
    A: The specifics of the payment process will be negotiated with the specific vendor chosen for the engagement.
40. If this SOW is requesting staff augmentation / "Time and Materials" services, are vendors still required to provide the following:
    Project Approach and Outcome:
    Describe the approach vendor will take to execute this work and ensuring all completion of all deliverables or additional work as deemed appropriate. The Vendor will submit an overview of what will comprise the completed learning experience. Vendor should also submit a high level timeline for the work.
    This information does not seem applicable for response to a staff augmentation position.
    A: This is not a staff augmentation engagement.
41. Please confirm that vendor assigned resource(s) will be working at the direction and under the supervision of a MNsure Project Manager.
    A: The vendor resources will report to state of MN, ultimately to the MNsure security governance committee.
42. Please confirm that vendor assigned resource(s) will be working at the direction and under the supervision of a MNsure Project Manager.
    A: The vendor resources will report to state of MN, ultimately to the MNsure security governance committee of which I am the chair.
43. Is there an incumbent vendor who is currently, or has previously, been engaged to perform duties similar to the work outlined in this SOW?
44. If yes, who is the incumbent vendor and will they be permitted to respond to this SOW?
    A: The state has retained vendors to do general security assessment work in the past. MNsure is a new system, not yet deployed, and has not yet had any 3rd party security assessment.
45. What is the anticipated daily work schedule for selected vendor resource(s) (8AM - 5PM, Monday thru Friday)?
    A: This will likely be variable. The assessment team will need to put in appropriate time to get the work done.
46. Please confirm that the anticipated utilization of selected resource(s) will be full-time 40 hours per week (excluding State holidays) for the duration of the contract?
    If no, please provide anticipated utilization?
    A: The anticipated utilization is whatever it takes to get the work done.
47. Will selected vendor resource(s) be required to perform off-hours, on-call support work?

A: There is no support work associated with this engagement. This is strictly a security controls assessment.

48. Please confirm that MNsure will provide selected contractor resource(s) with the laptop/desktop computer, hardware, software, and peripherals needed to perform the duties outlined in this SOW.
    A: The proposal should include information on how the vendor plans to complete the engagement. If laptop/desktop, hardware, software or any other materials are required for the vendor's proposed plan, this should be included in the proposal.
49. How many contractor resources does MNsure anticipate selecting and needing to perform the duties outlined in this SOW?
    A: The work must be completed within the listed timeframes. We expect the vendor to be familiar with these kinds of engagements and propose a team size needed to complete the work and meet the requirements in the SOW.
50. It seems the dates for the dates for deliverables do not directly align with the Project Milestones and Schedule (e.g., the Gap Assessment Report Deliverable is under the August 2013 timeframe, whereas the Gap Assessment start date is November in the schedule). Could you please clarify the dates for each?
    A: The timeline in the SOW is correct. The first mention of "gap" is in the November timeframe. The SOW is for a 3-part engagement: 1. Initial assessment in Jul-Aug; 2. Gap/remediation assessment in Nov/Dec, and; 3. Re-assessment of updated system in Mar-Jun 2014.
51. Does the one reference required for the proposal submission mean one reference for a project that the company has performed or one reference for each key personnel submitted?
    A: The state expects that submitting vendors will have experience with similar assessments. If the proposed assessment team has worked on these previous engagements then a single reference who can speak to this is sufficient. If the vendor is putting together a new team for this engagement, who have not worked together on similar assessments with the vendor then it might not be possible to provide one reference. The state is expecting vendors to put forth their "A" team for this engagement – a team that has worked together on similar engagements for that vendor.